UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/943,683	08/30/2001	Hideaki Watanabe	09792909-5124	9983

26263   7590   10/06/2005

SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. BOX 061080
WACKER DRIVE STATION, SEARS TOWER
CHICAGO, IL 60606-1080

EXAMINER
ELMORE, JOHN E

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 10/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _19 July 2005_.

2a)☒ This action is **FINAL.**   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-30_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-30_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _30 August 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some *   c)☐ None of:

        1.☒ Certified copies of the priority documents have been received.

        2.☐ Certified copies of the priority documents have been received in Application No. _____.

        3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   In response to the previous office action, Applicant has amended claims 1, 14,

16, 17 and 30. Claims 1-30 have been examined.

Objections to Specification

2.   In view of Applicant's amendment, the previous objections to the specification are

withdrawn.

Claim Rejections - 35 USC § 112

3.   In view of Applicant's amendment, the previous rejections under 25 U.S.C. 112

are withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1.   **Claims 1, 8, 9, 14-16 and 30 are rejected under 35 U.S.C. 103(a)** as being

unpatentable over Dulude et al. (US 6,310,966), hereafter Dulude, in view of Bianco et

al. (US 6,256,737), hereafter Bianco,

Regarding claim 1, Dulude teaches an authentication system comprising:

a person identification authority (registration authority 34) which creates a person

identification certificate (biometric certificate 68) for storing the template (registration

biometric data) and which issues the person identification certificate to an entity which

executes person authentication, wherein said person identification authority acquires

the template and data for person identification from the user to be certified with the

person identification certificate, and encrypts the template using a key and creates and

registers on the basis of the identification of the user, the person identification certificate

for storing the template which is the person identification data (certifying authority

acquires the template and encrypts it using col. 4, lines 13-32; col. 5, lines 33-40; col. 6,

lines 32-34), and

the entity which decrypts the encrypted template stored in the person

identification certificate and executes person authentication (reception section 42)

compares the template stored in the person identification certificate with the sampling

information of the user so as to execute person authentication (Fig. 5; col. 7, lines 33-

44).

But Dulude does not explain that the key with which the certifying authority

encrypts the template is a public key.

However, Bianco teaches an authentication system wherein a biometric template

(502) is encrypted by a person identification authority (biometric server 104) using the

public key of the entity which executes person authentication (identity device module

2908) for the purpose of providing additional security in the authentication of users by

securing communication of the template (col. 55, line 47-col. 56, line 67).

Therefore, it would be obvious to one of ordinary skill in the art to provide that the person identification authority encrypts the template using a public key. One would be motivated to do so in order to provide additional security in the authentication of users, particularly where the template is transmitted over an unsecure network from the person identification authority to an entity which executes person authentication.

Regarding claim 8, the modified system of Dulude and Bianco is relied upon as applied to claim 1, and Dulude and Bianco further teach that said person identification authority issues, in response to a request from the entity which executes person authentication, the registered person identification certificate to the entity, and in the issuing of the person identification certificate to the entity, the template to be stored in the person identification certificate is issued as an encrypted data which may be decrypted in the entity (col. 6, lines 58-65). Therefore, for the reasons provided above, such a claim also would be obvious.

Regarding claim 9, the modified system of Dulude and Bianco is relied upon as applied to claim 1, and Dulude and Bianco further teach that said person identification authority issues, in response to a request from the entity which executes person authentication, the registered person identification certificate to the entity, and in the issuing of the person identification certificate to the entity, the template to be stored in the person identification certificate is issued as data encrypted with a public key of the entity (col. 6, lines 58-65). Therefore, for the reasons provided above, such a claim also would be obvious.

Regarding claim 14, the modified system of Dulude and Bianco is relied upon

as applied to claim 1, and Dulude and Bianco further teach that template to be stored in

the person identification certificate created by said person identification authority

comprises biometric information of a person selected from the group consisting of

fingerprint information, retina pattern information, iris pattern information, voice print

information; non-biometric information, or any combination of two or more of the

biometric information and the non-biometric information selected from the group

consisting of a seal impression, a passport, a driver's license, and a credit card; any

combination of two or more of the biometric information and non-biometric information;

or any combination of any of the biometric or non-biometric information and a password

(biometric information including fingerprint, iris pattern, and retina pattern information;

col. 4, lines 33-42). Therefore, for reasons provided above, such a claim also would be

obvious.

Regarding claim 15, the modified system of Dulude and Bianco is relied upon

as applied to claim 1, and Dulude and Bianco further teach that the person identification

certificate issued by said person identification authority includes the digital signature

written by said person identification authority (Fig. 2; col. 4, lines 61-63). Therefore, for

reasons provided above, such a claim also would be obvious.

Regarding claim 16, the modified system of Dulude and Bianco is relied upon

as applied to claim 1, and Dulude and Bianco further teach that the entity is a service

provider which provides services to the user identified by the person identification

certificate, a user device that the user identified by the person identification certificate

accesses, or said person identification authority (receiving section 42 is a service provider to user; col. 8, lines 32-45, incorporating Vaeth, US 6,035,402; see Vaeth, col. 6, lines 5-26). Therefore, for reasons provided above, such a claim also would be obvious.

Regarding claims 17 and 24-25, this is a method version of the claimed system discussed above (claims 1 and 8-9). Therefore, for reasons provided above, such claims also would be obvious.

Regarding claim 30, this is a program-providing-medium version of the claimed system discussed above (claim 1). Therefore, for reasons provided above, such a claim also would have been obvious.

2.   **Claims 2-6, 10, 11, 18-22 and 26-27 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Dulude in view of Bianco, and further in view of Arnes ("Public Key Certification Revocation Schemes," Masters Thesis, Queen's University, February 2000).

Regarding claim 2, the modified system of Dulude and Bianco is relied upon as applied to claim 1, but Dulude and Bianco do not explain that said person identification authority acquires a template deleting request and the data for person identification from the user to be certified with the person identification certificate, deletes the template from the person identification certificate and registers the person identification certificate in a revocation list, on the basis of the identification of the user.

However, Arnes teaches a public key infrastructure wherein a person

identification authority (CA) acquires a certificate deleting request and the data for

person identification from the user to be certified with the person identification certificate

and registers the person identification certificate in a revocation list (CRL), on the basis

of the identification of the user for the purpose of revoking a certificate in response to a

change to the user's identifying information or a change in the relationship of the user

and the certifying authority (page 8, paragraphs 3 and 4). Arnes also teaches the

deletion of information contained in certificate prior to inclusion in a revocation list which

is unnecessary to prove revocation status for the purpose of reducing network load

(page 9, paragraph 3).

Therefore, it would be obvious to one of ordinary skill in the art at the time the

invention was made to modify the device of Dulude and Bianco with the teaching of

Arnes to provide that said person identification authority acquires a template deleting

request and the data for person identification from the user to be certified with the

person identification certificate, deletes the template from the person identification

certificate and registers the person identification certificate in a revocation list, on the

basis of the identification of the user. One would be motivated to do so in order to

revoke a certificate upon a change to the user's identifying information or a change in

the relationship of the user and the certifying authority and to process the revocation

with minimal impact on network load.

Regarding claim 3, this is the same as claim 2 except that the person

identification authority acquires a changing request along with a new template instead of

a deleting request. Arnes teaches the revocation of a certificate in response to a

changing request (e.g. change of subject name; page 8, paragraph 3). The Examiner

takes official notice that one of ordinary skill in the art at the time the invention was

made would recognize that the certification process regarding the change of the

template information is equivalent to the change of any other user information

associated with the certificate (e.g. name) and that the new information must be

provided along with the request; that is, the old certificate would be revoked and a new

certificate would be issued containing the updated information. Therefore, for the

reasons provided above, such a claim also would be obvious.

Regarding claim 4, this is the same as claim 3 except that the person

identification authority acquires an addition request instead of a changing request. One

of ordinary skill in the art at the time the invention was made would recognize that the

requests are functionally equivalent; that is, the authority receives a new template in

either case, and the addition request is equivalent to a change request that results in a

net addition of template information. Put another way, the addition of a new template is

equivalent to the replacement of the old template with a new template containing both

the old and new information. Therefore, for the reasons provided above, such a claim

also would be obvious.

Regarding claim 5, this is the same as claim 2 except that the person

identification authority acquires a suspension request instead of a deleting request and

invalidates rather than deletes the template. The Examiner takes official notice that one

of ordinary skill in the art at the time the invention was made would recognize the

alternative practice of flagging user information in a database as invalid instead of deleting that same information for the purpose of preserving the information where it is likely to be used again in the future, particularly where a user will likely be issued a new certificate based on the same information. Therefore, for the reasons provided above, such a claim also would be obvious.

Regarding claim 6, this is the same as claim 5 except that the person identification authority acquires a template suspension cancel request rather than a suspension request from the user and the subsequent steps are reversed. The Examiner takes official notice that one of ordinary skill in the art at the time the invention was made would recognize that the cancellation of a previous action involves a reversal of the steps involved to perform that action; that this, the template that was invalidated is re-validated and the person identification certificate that was placed in the revocation list is removed from the list. Therefore, for reasons provided above, such a claim also would be obvious.

Regarding claim 10, this is the same as claim 3 except that the person identification authority does not acquire a new template in association with the issuance of a new certificate. One of ordinary skill in the art at the time the invention was made would recognize that updating a certificate by issuing a new certificate containing the same template information as the old certificate is equivalent to a making a changing request and providing the same template information as contained in the old certificate. It would be obvious to one of ordinary skill in the art at the time the invention was made to eliminate the step of sending along the same template information for the issuance of

a new certificate for the motivation of reducing network load. Therefore, for reasons provided above, such a claim also would be obvious.

Regarding claim 11, the modified system of Dulude and Bianco is relied upon as applied to claim 1, but Dulude and Bianco do not explain that said person identification authority acquires a request for deleting the person identification certificate and the data for person identification from the user to be certified with the person identification certificate, deletes the person identification certificate, and requests deletion of the issued person identification certificate to the entity to which the person identification certificate is issued, on the basis of the identification of the user.

However, Arnes teaches a public key infrastructure wherein a person identification authority (CA) acquires a certificate deleting request and the data for person identification from the user to be certified with the person identification certificate and requests deletion of the issued person identification certificate to the entity to which the person identification certificate is issued, on the basis of the identification of the user for the purpose of revoking a certificate in response to a change to the user's identifying information or a change in the relationship of the user and the certifying authority (page 8, paragraph 3, through page 9, paragraph 2).

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Dulude and Bianco with the teaching of Arnes to provide said person identification authority acquires a request for deleting the person identification certificate and the data for person identification from the user to be certified with the person identification certificate, deletes the person identification

certificate, and requests deletion of the issued person identification certificate to the

entity to which the person identification certificate is issued, on the basis of the

identification of the user. One would be motivated to do so in order to revoke a

certificate upon a change to the user's identifying information or a change in the

relationship of the user and the certifying authority.

Regarding claims 18-22 and 26-27, this are a method version of the claimed

system discussed above (claims 2-6 and 10-11). Therefore, for reasons provided

above, such claims also would be obvious.

3.   **Claims 7, 13, and 29 are rejected under 35 U.S.C. 103(a)** as being

unpatentable over Dulude in view of Bianco, and further in view of Diffie et al., hereafter

Diffie, ("Authentication and Authenticated Key Exchanges," Designs, Codes and

Cryptography, Kluwer Academic Publishers, 1992).

Regarding claim 7, Dulude teaches all the limitations of claim 1, and further

teaches that the user to be certified with the person identification certificate requests

registration, deletion, change, addition, suspension, or canceling of suspension of the

template (e.g. registration request initiated by user device; col. 4, lines 12-65).

But Dulude does not explain that said person identification authority executes

mutual authentication with a user device in data communication with the user device,

and prevents and verifies data-tampering by creating a digital signature and performing

signature verification.

However, Diffie teaches a method of two-party mutual authentication wherein the parties exchange digital signatures (page 9, first paragraph) in addition to their public cryptographic keys for the purpose of enhancing security by assuring that each of the parties exchanging a public key is authentic and not an imposter (page 2, paragraph 3).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Dulude with the teaching of Diffie such that said person identification authority executes mutual authentication with a user device in data communication with the user device, and prevents and verifies data-tampering by creating a digital signature and performing signature verification. One would be motivated to do so in order to enhance network security by assuring that each of the parties exchanging a public key is authentic and not an imposter.

Regarding claim 13, Dulude teaches all the limitations of claim 1, and further teaches that person identification authority engages in data communication with the entity which executes person authentication, performed to issue, update, delete, or inquire the person identification certificate to the entity which executes person authentication (e.g. issue of a certificate; col. 4, lines 55-65; col. 5, lines 33-44; col. 6, lines 28-34).

But Dulude does not explain that said person identification authority executes mutual authentication with a device of the entity and verifies data validity by checking whether the data is tampered with by adding the digital signature and performing signature verification.

However, Diffie teaches a method of two-party mutual authentication wherein the parties exchange digital signatures (page 9, first paragraph) in addition to their public cryptographic keys for the purpose of enhancing security by assuring that each of the parties exchanging a public key is authentic and not an imposter (page 2, paragraph 3).

Therefore, it would be obvious to a person of ordinary skill in the computer art at the time the invention was made to modify the system of Dulude with the teaching of Diffie such that said person identification authority executes mutual authentication with a device of the entity and verifies data validity by checking whether the data is tampered with by adding the digital signature and performing signature verification. One would be motivated to do so in order to enhance network security by assuring that each of the parties exchanging a public key is authentic and not an imposter.

Regarding claim 29, this is a method version of the claimed system discussed above (claim 13). Therefore, for reasons provided above, such a claim also would have been obvious.

4.   **Claims 12 and 28 are rejected under 35 U.S.C. 103(a)** as being unpatentable over Dulude in view of Bianco, and further in view of Yu et al. (US 5,930,804), hereafter Yu.

Regarding claim 12, Dulude teaches all the limitations of claim 1, and further teaches that in the comparison for verification of the person identification certificate to the entity, the sampling information received is compared with the template in the

person identification certificate stored in said person identification authority, and a

comparison result is provided as a response (col. 6, lines 32-35; col. 7, lines 33-44).

But Dulude does not explain that the person identification authority performs

comparison for verification based on the person identification certificate in response to a

request from the entity which executes person authentication.

However, Yu teaches an authentication system wherein the person identification

authority (authentication center 24) performs comparison for verification based on the

person identification certificate in response to a request from the entity which executes

person authentication (web server 20, in response to request for service by user at web

client 14, requests verification from authentication center 24; Fig. 1 and 4; col. 8, lines 9-

20) for the purpose of providing a more secure and improved authentication system

(col. 2, lines 55-58).

Therefore, it would be obvious to a person of ordinary skill in the computer art at

the time the invention was made to modify the system of Dulude with the teaching of Yu

such that the person identification authority performs comparison for verification based

on the person identification certificate in response to a request from the entity which

executes person authentication. One would be motivated to do so in order to provide a

more secure and improved authentication system.

Regarding claim 28, this is a method version of the claimed system discussed

above (claim 12). Therefore, for reasons provided above, such a claim also would have

been obvious.

Conclusion

5.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

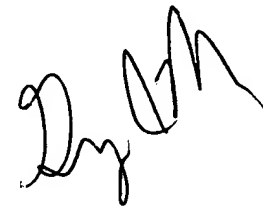than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to John Elmore whose telephone number is 571-272-4224.

The examiner can normally be reached on M 10-8, T-Th 9-7.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Greg Morse can be reached on 571-272-3838. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

John Elmore

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100